CLAIMS

What is claimed is:

1. A method of security enforcement for a persistent data repository comprising:

intercepting, in a nonintrusive manner, a data access transaction between a user application and a data repository having data items;

determining if the intercepted data access transaction corresponds to a security policy, the security policy indicative of restricted data items in the data repository to which the user application is prohibited access; and

limiting, based on the security policy, the data access transaction by modifying the data access transaction such that data indications, in the data access transaction, corresponding to restricted data items, according to the security policy, are modified in a resulting data access transaction.

2. The method of claim 1 wherein the security policy has rules, each of the rules including an object, a selection criteria and an action, the action indicative of restricted data items.

3. The method of claim 1 wherein the data indications are references to data items in the data repository and limiting further includes qualifying the references to generate a modified request indicative of unrestricted data items, such that successive retrieval operations employing the qualified references do not retrieve restricted data items.

4. The method of claim 3 wherein the data access transaction is a data access statement operative to request data and limiting further comprises:

'identifying at least one rule, according to the security policy, corresponding to the data access statement, the identified rule restricting access to at least one of the data items indicated by the data access statement; and

concatenating selection qualifiers to the data access statement corresponding to the identified rule, the selection qualifiers operable to omit the restricted data items from the qualified references of the data access statement.

5. The method of claim 1 wherein the data indications are rows of data retrieved from the data repository, and limiting further comprises:

identifying rows having restricted data items, and

eliminating the identified rows from the data access transaction such that the resulting data access transaction is a modified query response including rows without restricted data items.

6. The method of claim 5 wherein the data access transaction is a data query response including a row set and limiting further comprises:

comparing each of the rows in the row set to the rules of the security policy; and

selectively eliminating rows in the row set including the restricted data items, based on the comparing, to generate a modified query response including a filtered row set.

7. The method of claim 2 wherein the actions are selectively indicative of modifications, the modifications further comprising attributes, operators, and operands, the limiting further comprising

identifying data items corresponding to the attributes, each of the attributes associated with an operator and an operand;

applying an operator specified for the data item to the operand specified for the data item; and

determining, as a result of applying the operator, whether to eliminate the identified data item.

8. The method of claim 1 wherein the nonintrusive manner is undetectable to the user application and undetectable to the data repository.

9. The method of claim 1 wherein intercepting the data access transaction further comprises:

establishing a proxy to the data repository on behalf of the user;

receiving the data access transaction as a row set under the proxy; and wherein limiting includes:

regenerating the resulting data access transaction as a reduced row set having a subset of the rows from the proxy row set; and

transmitting the reduced row set to the user on behalf of the proxy.

10. The method of claim 1 wherein limiting the data access transaction further includes

receiving a set of packets, the packets encapsulating the data access transaction according to layered protocols;

interrogating and modifying the packets in a nondestructive manner with respect to the layered protocols; and

padding the packets for accommodating elimination of the restricted data items to generate the resulting data access transaction.

11. The method of claim 10 wherein generating the resulting data access transaction preserves the encapsulating layered protocol associating the packets without employing a proxy for regenerating the sequence of packets.

12. The method of claim 4 wherein intercepting the data access statement includes receiving an SQL query and limiting includes appending conditional selection statements to the SQL query, the conditional selection statements computed from the security policy, to generate the resulting data access transaction.

13. The method of claim 12 further comprising:

building a parse tree corresponding to the SQL query;

adding nodes in the parse tree corresponding to the appended conditional selection statements; and

reprocessing the parse tree to generate the resulting data access transaction.

14. The method of claim 6 wherein intercepting the data query response further comprises:

intercepting the data query response from the data repository as the data access transaction, the data query response encapsulated as a row set having rows from a relational database query, and further wherein limiting includes discarding rows in the row set having restricted data items and transmitting the remaining rows to the user as the resulting data access transaction.

15. The method of claim 1 wherein the nonintrusive manner is such that the intercepting and limiting occurs undetectable to both the source and the destination of the data access transaction.

16. The method of claim 1 wherein intercepting further comprises:

establishing an identification exchange intended for interception and operable to transmit an identification token indicative of an application user; and

parsing, as part of the intercepting, the identification exchange to extract the identification token, wherein the identification exchange is benign to the data repository.

17. The method of claim 1 wherein intercepting occurs in a data path between a source of the data access transaction and a destination of the resulting data access transaction, and limiting occurs in a component separate from the source and destination.

18. The method of claim 17 wherein the component separate from the source and destination is a separate network device than the components corresponding to the source and destination

19. The method of claim 1 wherein the restricted data items are eliminated from the resulting data access transaction.

20. A method for nonintrusive implementation of data level security enforcement comprising:

defining a security policy between an application and a data repository, the security policy having rules indicative of restricted data items, the rules associated with attributes and conditions;

identifying an entry point between the data repository and the application;

deploying a security filter at the entry point, the security filter operable to receive data manipulation messages between the application and the data repository; the security filter further operable to limit data exposure by the data repository by selectively modifying the data manipulation messages into conformance with the security policy, the limiting further comprising:

sniffing the entry point to determine data manipulation messages;

intercepting the sniffed data manipulation messages in a nondestructive manner;

comparing the sniffed messages to the rules in the security policy to determine if the sniffed data manipulation message includes restricted data items;

determining if the sniffed messages match at least one of the rules of the security policy;

selectively modifying, if the determining indicates a match between the rules and the data manipulating message, the data manipulation message to remove the matching restricted data item.

21. The method of claim 20 wherein determining comprises comparing attributes of the data manipulation messages with operators and operands in the compared rules, the operators and operands indicative of restricted data items in the data repository.

22. The method of claim 20 wherein modifying further comprises:

reconstructing a request query corresponding to a query syntax; and

adding limiters to the request query corresponding to the matching rules of the security policy, the adding performed in a nondestructive manner such that the modification is undetectable to the data repository.

23. The method of claim 20 wherein modifying further comprises:

identifying a data retrieval response encapsulated in a layered protocol on the data manipulation message; and

reconstructing the data retrieval response by deleting restricted data items from the data retrieval response, the reconstructing performed in a nondestructive manner undetectable to the application and conforming to the encapsulating layered protocol.

24. A data security filter device for security enforcement for a persistent data repository comprising:

an interceptor in the security filter operable to intercept, in a nonintrusive manner, a data access transaction between a user application and a data repository having data items;

a security policy table responsive to the interceptor to determine if the intercepted data access transaction corresponds to the security policy table, the security policy table indicative of restricted data items in the data repository to which the user application is prohibited access; and

a limiter operable to limit, based on the security policy, the data access transaction by modifying the data access transaction such that data indications, in the data access transaction, corresponding to restricted data items, according to the security policy table, are modified in a resulting data access transaction.

25. The security filter of claim 24 wherein the security policy has table rules, each of the rules including an object, a selection criteria and an action, the action indicative of restricted data items.

26. The security filter of claim 24 wherein the data indications are references to data items in the data repository and the limiter is operable to qualifying the references to generate a modified request indicative of unrestricted data items, such that successive retrieval operations, from the data repository, employing the qualified references do not retrieve restricted data items.

27. The security filter of claim 26 wherein the data access transaction is a data access statement operative to request data, wherein:

the interceptor is operable identify at least one rule, according to the security policy, corresponding to the data access statement, the identified rule restricting access to at least one of the data items indicated by the data access statement; and

the limiter is operable to concatenate selection qualifiers to the data access statement corresponding to the identified rule, the selection qualifiers operable to omit the restricted data items from the qualified references of the data access statement.

28. The security filter of claim 24 wherein the data indications are rows of data retrieved from the data repository, wherein:

the interceptor is operable to identify rows having restricted data items, and

the limiter is operable to eliminate the identified rows from the data access transaction such that the resulting data access transaction is a modified query response including rows without restricted data items.

29. The security filter of claim 28 wherein the data access transaction is a data query response including a row set wherein:

the interceptor is operable to compare each of the rows in the row set to the rules of the security policy; and

the limiter is operable to selectively eliminate rows in the row set including the restricted data items, based on the comparing, to generate a modified query response containing a filtered row set.

30. The security filter of claim 25 wherein the actions are selectively indicative of modifications, the modifications further comprising attributes, operators, and operands, wherein the limiter is operable to:

identify data items corresponding to the attributes, each of the attributes associated with an operator and an operand;

apply an operator specified for the data item to the operand specified for the data item; and determine, as a result of applying the operator, whether to eliminate the identified data item.

31. The security filter of claim 24 wherein the security filter is operable to manipulate the resulting data access transaction in a nonintrusive manner such that modifications performed on the data access transaction are undetectable to the user application and undetectable to the data repository.

32. The security filter of claim 24 wherein the interceptor is operable to:

establish a proxy to the data repository on behalf of the user;

receive the data access transaction as a row set under the proxy; and wherein the limiter is operable to

regenerate the resulting data access transaction as a reduced row set having a subset of the rows from the proxy row set; and

transmit the reduced row set to the user on behalf of the proxy.

33. The security filter of claim 24 wherein the data access transaction is contained in a set of packets wherein the limiter is operable to:

receive the set of packets, the packets encapsulating the data access transaction according to layered protocols;

interrogate and modify the packets in a nondestructive manner with respect to the layered protocols; and

pad the packets for accommodating elimination of the restricted data items to generate the resulting data access transaction.

34. The security filter of claim 33 wherein the resulting data access transaction conforms to the encapsulating layered protocol associating the packets.

35. The security filter of claim 27 wherein the data access statement is an SQL query and wherein the limiter is operable to append conditional selection statements to the SQL

query, the conditional selection statements computed from the security policy, to generate the resulting data access transaction.

36. The security filter of claim 35 further comprising a parse tree, the interceptor operable to build the parse tree corresponding to the SQL query, wherein the limiter is further operable to add nodes to the parse tree corresponding to the appended conditional selection statements; and reprocessing the parse tree to generate the resulting data access transaction.

37. The security filter of claim 24 wherein the interceptor is operable to intercept the data query response from the data repository as the data access transaction, the data query response encapsulated as a row set having rows from a relational database query, wherein the limiter is operable to discard rows in the row set having restricted data items and transmit the remaining rows to the user as the resulting data access transaction.

38. The security filter of claim 24 wherein the user application and the data repository define a data path between a source of the data access transaction and a destination of the resulting data access transaction, wherein the security filter is disposed in a component separate from the source and destination.

39. The security filter of claim 38 wherein the component separate from the source and destination is a separate network device than the components corresponding to the source and destination

40. A method for nonintrusive implementation of data level security enforcement comprising

defining a security policy having rules, the rules further specifying attributes and conditions;

intercepting a data retrieval request;

comparing the data retrieval request to the security policy;

determining if the data retrieval request corresponds to at least one of the rules of the security policy;

identifying, via a parse tree, selectivity operators indicative of the data to be retrieved;

modifying the parse tree according to the corresponding rule to generate a modified data retrieval request; and

forwarding the modified data retrieval request to the data repository for subsequent retrieval and transport to the requesting user.

41. A computer program product having a computer readable medium operable to store computer program logic embodied in computer program code encoded thereon for implementing security enforcement in a persistent data repository comprising:

computer program code for intercepting, in a nonintrusive manner, a data access transaction between a user application and a data repository having data items;

computer program code for determining if the intercepted data access transaction corresponds to a security policy, the security policy indicative of restricted data items in the data repository to which the user application is prohibited access; and

computer program code for limiting, based on the security policy, the data access transaction by modifying the data access transaction such that data indications, in the data access transaction, corresponding to restricted data items, according to the security policy, are modified in a resulting data access transaction.

42. A computer data signal having program code for security enforcement for a persistent data repository comprising:

program code for intercepting, in a nonintrusive manner, a data access transaction between a user application and a data repository having data items;

program code for determining if the intercepted data access transaction corresponds to a security policy, the security policy indicative of restricted data items in the data repository to which the user application is prohibited access; and

program code for limiting, based on the security policy, the data access transaction by modifying the data access transaction such that data indications, in the data access transaction, corresponding to restricted data items, according to the security policy, are modified in a resulting data access transaction.

43. A data security filter device for security enforcement for a persistent data repository comprising:

means for intercepting, in a nonintrusive manner, a data access transaction between a user application and a data repository having data items;

means for determining if the intercepted data access transaction corresponds to a security policy, the security policy indicative of restricted data items in the data repository to which the user application is prohibited access; and

means for limiting, based on the security policy, the data access transaction by modifying the data access transaction such that data indications, in the data access transaction, corresponding to restricted data items, according to the security policy, are modified in a resulting data access transaction.